PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-341337
(43)Date of publication of application : 08.12.2000

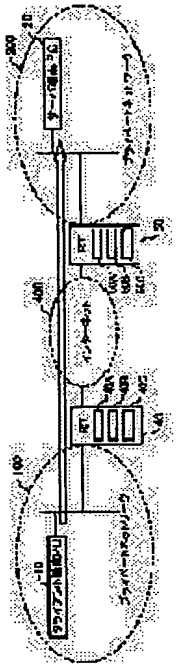
(51)Int.Cl. H04L 12/56
H04L 12/46
H04L 12/28
H04L 12/66

(21)Application number : 11-153248
(22)Date of filing : 01.06.1999

(71)Applicant : NEC CORP
(72)Inventor : SATO TAKESHI

(54) INTER-PRIVATE-NETWORK CONNECTION SYSTEM AND ITS METHOD BY IP MASQUERADE

(57)Abstract:
PROBLEM TO BE SOLVED: To effectively utilize a global IP address.
SOLUTION: The inter-private-network connection system by an IP masquerade to connect private networks with an IP masquerade function via the Internet is provided with routers 40, 50 that are placed to each private network and have an OP masquerade function. The router 40(50) has a port number reservation table 40C(50C) that stores in common a plurality of reservation host names for the terminals requesting connection in advance and a plurality of internal recognition port numbers corresponding to the reservation host names respectively, each router references the port number reservation table and uses an internal reservation port number for a sender port number of a packet in the case of connection to the Internet, recognizes a reservation host name from the internal reservation port number used for the packet sender port number in the case of connection to the private network, and gives the packet to the terminal with the recognized reservation host name.



LEGAL STATUS

[Date of request for examination] 23.05.2000
[Date of sending the examiner's decision of rejection] 12.10.2001
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－341337
（P2000－341337A）
(43)公開日　平成12年12月８日(2000.12.8)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｈ０４Ｌ 12/56		Ｈ０４Ｌ 11/20	１０２Ｄ	５Ｋ０３０
12/46		11/00	３１０Ｃ	５Ｋ０３３
12/28		11/20	Ｂ	９Ａ００１
12/66				

審査請求　有　　請求項の数９　ＯＬ　（全 10 頁）

(21)出願番号　特願平11－153248

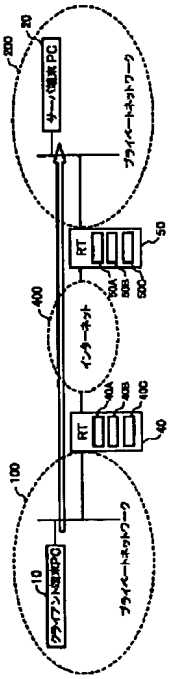
(22)出願日　平成11年６月１日(1999.6.1)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　佐藤　壮
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100104400
弁理士　浅野　雄一郎

Ｆターム(参考)　5K030 GA04 GA19 HB11 HB28 HC01 HD03 HD06 HD09 JT06 KA05
5K033 AA04 CB08 CC01 DA06 DB12 DB19 EC03
9A001 BB04 CC08 EE02 JJ25 KK31 LL03

(54)【発明の名称】　ＩＰマスカレードによるプライベートネットワーク間接続システム及び方法

(57)【要約】
【課題】　グローバルＩＰアドレスの有効活用を可能にする。
【解決手段】　インターネットを介してプライベートネットワーク間をＩＰマスカレード機能で接続するためのＩＰマスカレードによるプライベートネットワーク間接続システムに、プライベートネットワークの各々に設けられ、ＩＰマスカレード機能を有するルータ40,50を備え、ルータは、予め接続が要求される端末の複数の予約ホスト名、予約ホスト名の各々に対応する複数の内部予約ポート番号を各ルータで共通に保持するポート番号予約テーブル40C,50Cを有し、ルータは、ポート番号予約テーブルを参照して、インターネットへの接続時に、、パケットの送信元ポート番号として内部予約ポート番号を用い、プライベートネットワークへの接続時に、パケットの送信元ポート番号として用いられた内部予約ポート番号から予約ホスト名を認識して、認識された予約ホスト名の端末にパケットを渡す。



【特許請求の範囲】
【請求項１】　インターネットを介してプライベートネットワーク間をＩＰマスカレード機能で接続するためのＩＰマスカレードによるプライベートネットワーク間接続システムにおいて、
前記プライベートネットワークの各々に設けられ、ＩＰマスカレード機能を有するルータを備え、前記ルータは、
予め接続が要求される端末の複数の予約ホスト名、前記予約ホスト名の各々に対応する複数の内部予約ポート番号を各ルータで共通に保持するポート番号予約テーブルを有し、
前記ルータは、前記インターネットへの接続時に、前記ポート番号予約テーブルを参照して、パケットの送信元ポート番号として前記内部予約ポート番号を用い、
前記ルータは、前記プライベートネットワークへの接続時に、前記ポート番号予約テーブルを参照し、パケットの前記送信元ポート番号として用いられた前記内部予約ポート番号から予約ホスト名を認識して、認識された前記予約ホスト名の端末に前記パケットを渡すことを特徴とするＩＰマスカレードによるプライベートネットワーク間接続システム。
【請求項２】　前記ルータの各々は、ＤＨＣＰ機能を用いて前記端末がサーバ機能を有するものに予約ホスト名を割当て、さらに、ＤＮＳ機能を用いてテーブル前記インターネットを介して対向する前記ルータに相互に予約ホスト名を問い合わせて、前記ポート番号予約テーブルが共通の予約ホスト名を保持することを可能にすることを特徴とする、請求項１に記載のＩＰマスカレードによるプライベートネットワーク間接続システム。
【請求項３】　前記ポート番号予約テーブルは、複数の前記内部予約ポート番号に対応して仮ＩＰアドレスを各ルータで個別に保持し、パケットの送信先プライベートＩＰアドレスとして前記仮ＩＰアドレスが用いられるようにすることを特徴とする、請求項１に記載のＩＰマスカレードによるプライベートネットワーク間接続システム。
【請求項４】　前記インターネットへの接続時に、前記ポート番号予約テーブルを参照し、前記ルータは、パケットの送信元ポート番号の番号を、パケットの送信先プライベートＩＰアドレスとして用いた前記仮ＩＰアドレスに対応する内部予約ポート番号に変換することを特徴とする、請求項３に記載のＩＰマスカレードによるプライベートネットワーク間接続システム。
【請求項５】　前記送信元ポート番号は、パケットの送信先プライベートＩＰアドレスとして用いた前記仮ＩＰアドレスに対応して前記ポート番号予約テーブルに保持されることを特徴とする、請求項４に記載のＩＰマスカレードによるプライベートネットワーク間接続システム。
【請求項６】　前記ポート番号予約テーブルはパケットの送信先プライベートＩＰアドレスとして用いた前記仮ＩＰアドレスに対応して送信先グローバルＩＰアドレスを保持することを特徴とする、請求項３に記載のＩＰマスカレードによるプライベートネットワーク間接続システム。
【請求項７】　前記ポート番号予約テーブルに保持されている内容が一定期間使用されていない場合にはその内容を削除することを特徴とする、請求項１に記載のＩＰマスカレードによるプライベートネットワーク間接続システム。
【請求項８】　前記プライベートネットワーク間の接続は、広域ネットワーク、インターネットを介して行われることを特徴とする、請求項１に記載のＩＰマスカレードによるプライベートネットワーク間接続システム。
【請求項９】　インターネットを介してプライベートネットワーク間をＩＰマスカレード機能で接続するためのＩＰマスカレードによるプライベートネットワーク間接続方法において、
前記プライベートネットワークの各々にルータを設けて、前記ルータにＩＰマスカレード機能をサポートさせる工程と、
予め接続が要求される端末の複数の予約ホスト名、前記予約ホスト名の各々に対応する複数の内部予約ポート番号を各ルータのポート番号予約テーブルで共通に保持する工程と、
前記ルータは、前記インターネットへの接続時に、前記ポート番号予約テーブルを参照して、パケットの送信元ポート番号として前記内部予約ポート番号を用いる工程と、
前記ルータは、前記プライベートネットワークへの接続時に、前記ポート番号予約テーブルを参照し、パケットの前記送信元ポート番号として用いられた前記内部予約ポート番号から予約ホスト名を認識して、認識された前記予約ホスト名の端末に前記パケットを渡す工程を備えることを特徴とするＩＰマスカレードによるプライベートネットワーク間接続方法。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明はＩＰマスカレードによるプライベートネットワーク間接続システム及び方法に関する。特に、本発明は、グローバルＩＰアドレス入手の削減、ＷＡＮ回線契約チャンネル数の削減が図れるＩＰマスカレードによるプライベートネットワーク間接続システム及び方法に関する。
【０００２】
【従来の技術】図５は従来のＩＰマスカレードによるプライベートネットワーク間接続システムを説明する図である。なお、全図を通して同一の構成要素には同一の符号、記号を用いる。本図に示すように、プライベートネ

ットワーク100、200は、WAN（Wide Area Network；広域ネットワーク）回線300に接続され、さらにWAN回線300を介してインターネット400に接続されている。WAN回線300には、例えば、ISDN（Integrated Service Digital Network；総合デジタルサービス網）、ATM（Asynchronous Transfer Mode；非同期転送モード）が適用されていてもよい。

【0003】プライベートネットワーク100にはクライアント端末PC1（Personal Computer）、インターネット400にはサーバ端末PC3が接続され、プライベートネットワーク200にはサーバ端末PC2が接続されているとする。インターネット400にはインターネットサービスプロバイダーが所有するゲートウエイISP6、7が設けられ、ゲートウエイISP6、7はWAN400とインターネット400との間の緩衝を果たす。

【0004】プライベートネットワーク100、200にはルータ4、5が設けられ、パケットの行き先案内を行う。なお、パケットはIPアドレスとデータとからなり、IPアドレスはデータの送信元IPアドレスとデータの送信先IPアドレスとからなる。ルータ4はIP（Internet Protocol）マスカレード（Masqerade）機能をサポートする。マスカレード機能はプライベートネットワーク100内にプライベートIPアドレスを有するクライアント端末PC1の複数が同時にインターネット400に同時に接続要求を行うと、パケットの複数送信元のプライベートIPアドレスを1つのグローバルIPアドレスに変換し、個々の接続要求はポート番号で区別される。

【0005】このようにして、プライベートネットワーク100からインターネット400に要求するクライアント端末PC1の複数の同時接続が1つのグローバルIPアドレスで可能になる。他方、ルータ5はNAT（Network Address Translation）機能をサポートする。NAT機能はプライベートIPアドレスとグローバルIPアドレスとを1対1で相互に変換する機能である。プライベートネットワーク200内にプライベートIPアドレスを有するサーバ端末2が複数存在する場合、サーバ端末2の複数へのパケットでは複数宛先のグローバルIPアドレスの各々がプライベートIPアドレスに変換される。このようにして、インターネット400からプライベートネットワーク200に要求されるサーバ端末PC2の複数の同時接続が可能になる。

【0006】

【発明が解決しょうとする課題】しかしながら、従来の上記IPマスカレードによるプライベートネットワーク間接続システムのプライベートネットワーク200では、グローバルIPアドレスを必要とするサーバ端末PC2の数だけインターネットプロバイダーからグローバルIPアドレスを入手する必要があるという第1の問題が発生する。すなわち、グローバルIPアドレスの有効活用を図る必要がある。

【0007】サーバ端末2がインターネット400を経由せず、直接にWAN回線300を経由するイントラネット接続によれば、グローバルIPアドレスの入手の問題は解決する。しかし、プライベートネットワーク100からWAN回線300を経由してインターネット400へのチャンネルと、プライベートネットワーク100からWAN回線300を経由してクライアントネットワーク200へのチャンネル、計2チャンネルのWAN回線を契約する必要があるという第2の問題が発生する。

【0008】したがって、本発明は上記問題点に鑑みて、グローバルIPアドレスを1つ入手するだけで、インターネットとイントラネットの同時接続を可能にし、WAN回線を1チャンネルに削減することを可能にするIPマスカレードによるプライベートネットワーク間接続システム及び方法を提供することを目的とする。

【0009】

【課題を解決するための手段】本発明は前記問題点を解決するために、インターネットを介してプライベートネットワーク間をIPマスカレード機能で接続するためのIPマスカレードによるプライベートネットワーク間接続システムにおいて、前記プライベートネットワークの各々に設けられ、IPマスカレード機能を有するルータを備え、前記ルータは、予め接続が要求される端末の複数の予約ホスト名、前記予約ホスト名の各々に対応する複数の内部予約ポート番号を各ルータで共通に保持するポート番号予約テーブルを有し、前記ルータは、前記インターネットへの接続時に、前記ポート番号予約テーブルを参照して、パケットの送信元ポート番号として前記内部予約ポート番号を用い、前記ルータは、前記プライベートネットワークへの接続時に、前記ポート番号予約テーブルを参照し、パケットの前記送信元ポート番号として用いられた前記内部予約ポート番号から予約ホスト名を認識して、認識された前記予約ホスト名の端末に前記パケットを渡すことを特徴とするIPマスカレードによるプライベートネットワーク間接続システムを提供する。

【0010】この手段により、IPマスカレード機能によりプライベートネットワークからインターネットへの同時接続時には1つのグローバルIPアドレスがあればよく、ポート番号予約テーブルを参照することによりインターネットからプライベートネットワークへの同時接続時にも1つのグローバルIPアドレスがあればよいので、グローバルIPアドレスの有効活用が可能である。好ましくは、前記ルータの各々は、DHCP機能を用いて前記端末がサーバ機能を有するものに予約ホスト名を

割当て、さらに、ＤＮＳ機能を用いてテーブル前記インターネットを介して対向する前記ルータに相互に予約ホスト名を問い合わせて、前記ポート番号予約テーブルが共通の予約ホスト名を保持することを可能にする。

【００１１】この手段により、前記ルータの各々のポート番号予約テーブルではＤＨＣＰ機能、ＤＮＳ機能を用いてサーバとしてサービスを提供する端末の名を予約ホスト名が共通に容易に保持されることが可能になる。好ましくは、前記ポート番号予約テーブルは、複数の前記内部予約ポート番号に対応して仮ＩＰアドレスを各ルータで個別に保持し、パケットの送信先プライベートＩＰアドレスとして前記仮ＩＰアドレスが用いられるようにし、さらに、前記インターネットへの接続時に、前記ポート番号予約テーブルを参照し、前記ルータは、パケットの送信元ポート番号の番号を、パケットの送信先プライベートＩＰアドレスとして用いた前記仮ＩＰアドレスに対応する内部予約ポート番号に変換する。

【００１２】この手段により、インターネット接続時にパケットの送信元ポート番号の番号が内部予約ポート番号に変換されることにより、プライベートネットワーク接続時に変換された内部予約ポート番号が予約ホスト名に認識される。好ましくは、前記送信元ポート番号は、パケットの送信先プライベートＩＰアドレスとして用いた前記仮ＩＰアドレスに対応して前記ポート番号予約テーブルに保持される。この手段により、プライベートネットワークへの逆の接続時に、仮ＩＰアドレスに対応してパケットの送信先ポート番号は送信先プライベートＩＰアドレスに変換される。

【００１３】好ましくは、前記ポート番号予約テーブルはパケットの送信先プライベートＩＰアドレスとして用いた前記仮ＩＰアドレスに対応して送信先グローバルＩＰアドレスを保持する。この手段により、保持される送信先グローバルＩＰアドレスは送信すべき端末のプライベートネットワークについて１つである。すなわち、１つの送信先グローバルＩＰアドレスでプライベートネットワークに接続可能であるので、グローバルＩＰアドレスの活用が可能になる。好ましくは、前記ポート番号予約テーブルに保持されている内容が一定期間使用されていない場合にはその内容を削除する。

【００１４】この手段により、使用されていない予約ホスト名に関連する内容の堆積がなくなり、処理煩雑を回避できる。好ましくは、前記プライベートネットワーク間の接続は、広域ネットワーク、インターネットを介して行われる。この手段により、インターネット、イントラネットを同時に接続しても、広域ネットワークの契約は１回線でよい。

【００１５】さらに、本発明は、インターネットを介してプライベートネットワーク間をＩＰマスカレード機能で接続するためのＩＰマスカレードによるプライベートネットワーク間接続方法において、前記プライベートネットワークの各々にルータを設けて、前記ルータにＩＰマスカレード機能をサポートさせる工程と、予め接続が要求される端末の複数の予約ホスト名、前記予約ホスト名の各々に対応する複数の内部予約ポート番号を各ルータのポート番号予約テーブルで共通に保持する工程と、前記ルータは、前記インターネットへの接続時に、前記ポート番号予約テーブルを参照して、パケットの送信元ポート番号として前記内部予約ポート番号を用いる工程と、前記ルータは、前記プライベートネットワークへの接続時に、前記ポート番号予約テーブルを参照し、パケットの前記送信元ポート番号として用いられた前記内部予約ポート番号から予約ホスト名を認識して、認識された前記予約ホスト名の端末に前記パケットを渡す工程を備えることを特徴とするＩＰマスカレードによるプライベートネットワーク間接続方法を提供する。

【００１６】この手段により、上記本発明と同様に、ＩＰマスカレード機能によりプライベートネットワークからインターネットへの同時接続時には１つのグローバルＩＰアドレスがあればよく、ポート番号予約テーブルを参照することによりインターネットからプライベートネットワークへの同時接続時にも１つのグローバルＩＰアドレスがあればよいので、グローバルＩＰアドレスの有効活用が可能である。

【００１７】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。図１は本発明に係るＩＰマスカレードによるネットワーク構成を示す図である。本図では、説明の簡単化のために、図５におけるＷＡＮ回線３００を省略してある。本図に示すプライベートネットワーク１００、２００の各々に設けられるルータ４０、５０はＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ；動的ホスト構成プロトコル）機能、ＤＮＳ（Ｄｏｍａｉｎ Ｎａｍｅ Ｓｙｓｔｅｍ）機能、ＩＰマスカレード機能をサポートする。

【００１８】これらの機能のサポートに伴って、ルータ４０、５０には、ＤＨＣＰエントリーテーブル４０Ａ、５０Ａ、ＤＮＳエントリーテーブル４０Ｂ、５０Ｂ、ポート番号予約テーブル４０Ｃ、５０Ｃがそれぞれ実装される。プライベートネットワーク１００のクライアント端末ＰＣ１０の複数が同時にインターネット４００に接続要求してそのうちの全部又はいくつかがインターネット４００を経由してプライベートネットワーク２００に、以下のように、イントラネット接続を行う。

【００１９】図２はルータ４０、５０のＤＨＣＰ機能を説明する図である。本図に示すように、クライアント端末ＰＣ１０、サーバ端末ＰＣ２０、サーバ端末ＰＣ２１は、電源の投入後、ＤＨＣＰクライアント機能を使用して該当するＤＨＣＰサーバのルータ４０、５０に対してプライベートＩＰアドレスを要求する（本図の❶、❷、

③参照)。クライアントＩＤ（本図の場合、端末のホスト名）と割当プライベートＩＰアドレスの対応付けによりルータ４０、５０は該当するクライアント端末ＰＣ１０、サーバ端末ＰＣ２０、サーバ端末ＰＣ２１に対しプライベートＩＰアドレス：ａａａａ、ｄｄｄｄ、ｅｅｅｅをそれぞれ割当てる。

【００２０】

【表１】

ＲＴ４０のＤＨＣＰエントリーテーブル４０Ａ

ホスト名	プライベートＩＰアドレス	予約ホスト名
ＰＣ１０	a.a.a.a	－

【表２】

ＲＴ５０のＤＨＣＰエントリーテーブル５０Ａ

ホスト名	プライベートＩＰアドレス	予約ホスト名
ＰＣ２０	d.d.d.d	サーバ０１
ＰＣ２１	e.e.e.e	サーバ０２

【００２１】上記の表１、２に示すように、ルータ４０、５０のＤＨＣＰアドレスプール（割当てられるＩＰアドレスの束）には、ホスト名と割当ＩＰアドレスの対応エントリーが存在しこの他に「予約ホスト名」のエントリーが設定される。この予約ホスト名は該当する端末（ホスト名）が何らかの機能を提供するサーバを予めエントリーしておくもので、表２に示す予約ホスト名「サーバ０１」は、例えば、テルネット（Ｔｅｌｎｅｔ）サーバである。なお、テルネットは接続される相手のコンピュータを対話形式によって遠隔操作できるサービスである。

【００２２】また、表１の予約ホスト名は本発明の機能を使用する全てのルータで統一がとれている必要があり、ルータ４０、５０が収容している全てのクライアント端末ＰＣ１０、サーバ端末ＰＣ２０、サーバ端末ＰＣ２１のホスト名と重複しないように割当てられる。なお、クライアント端末ＰＣ１０、サーバ端末ＰＣ２０、サーバ端末ＰＣ２１は、ホスト名ＰＣ１０、ホスト名ＰＣ２０、ホスト名ＰＣ３０とそれぞれ名づけられる。また、ホスト名ＰＣ２０、ＰＣ２１に対して、表２に示すように、予約ホスト名はサーバ０１、サーバ０２のように名づけられる。

【００２３】具体的には、本図の①に示すように、クライアント端末ＰＣ１０からルータ４０に対してＤＨＣＰを探すためのパケット（ＤＨＣＰ　ＤＩＳＣＯＶＥＲ）が送信されると、ルータ４０はクライアント端末ＰＣ１０に応答パケット（ＤＨＣＰＯＦＦＥＲ）を送信してクライアント端末ＰＣ１０のアドレス；ａａａａを割当てる。同様に、本図の②に示すように、サーバ端末ＰＣ２０からルータ５０に対してＤＨＣＰを探すためのパケット（ＤＨＣＰ　ＤＩＳＣＯＶＥＲ）が送信されると、ルータ５０はサーバ端末ＰＣ２０に応答パケット（ＤＨＣＰ　ＯＦＦＥＲ）を送信してサーバ端末ＰＣ２０のアドレス；ｄｄｄｄを割当てる。

【００２４】同様に、本図の③において、サーバ端末ＰＣ２１からルータ５０に対してＤＨＣＰを探すためのパケット（ＤＨＣＰ　ＤＩＳＣＯＶＥＲ）が送信されると、ルータ５０はサーバ端末ＰＣ２１に応答パケット（ＤＨＣＰ　ＯＦＦＥＲ）を送信してサーバ端末ＰＣ２１のアドレス；ｅｅｅｅを割当てる。図３はルータ４０、５０のＤＮＳ機能を説明する図である。本図に示すサーバ端末ＰＣ２０がテルネット（Ｔｅｌｎｅｔ）サーバ機能を有し、クライアント端末ＰＣ１０がテルネットクライアント機能を有しているとする。

【００２５】また、クライアント端末ＰＣ１０のＤＮＳサーバ指定にルータ４０が設定されていたとし、さらに、ルータ４０のＤＮＳサーバ検索エントリーにルータ５０が指定されていたとする。また、ルータ４０、５０において、ＤＨＣＰのアドレスプールはＤＮＳエントリーテーブルに自動更新するようにしておく。これにより、ルータ４０、５０のＤＮＳエントリーテーブルは下記の表３、５のようになる。

【００２６】

【表３】

ＲＴ４０のＤＮＳエントリーテーブル４０Ｂ

（ＤＮＳ応答受信前）

ドメイン名	プライベートＩＰアドレス	予約ホスト名
ＰＣ10	a.a.a.a	－

【表４】

ＲＴ４０のＤＮＳエントリーテーブル４０Ｂ

（ＤＮＳ応答受信後）

ホスト名	プライベートＩＰアドレス	予約ホスト名
ＰＣ１０	a.a.a.a	－
ＰＣ２０	c.c.c.c	サーバ０１

【表５】

ＲＴ５０のＤＮＳエントリーテーブル５０Ｂ

ホスト名	プライベートＩＰアドレス	予約ホスト名
ＰＣ２０	d.d.d.d	サーバ０１
ＰＣ２１	e.e.e.e	サーバ０２

【００２７】ＤＨＰＣのアドレスプールと同じく、ルータ４０、５０はＤＮＳエントリーテーブルには、ドメイン名（説明を簡単にするために、ここではドメイン名（ＦＱＤＮ；Ｆｕｌｌｙ　Ｑｕａｌｉｆｉｅｄ　Ｄｏｍａｉｎ　Ｎａｍｅ）にホスト名を使用している）とＩＰ

アドレスとが存在しこの他に「予約ホスト名」のエントリーが設定される。例えば、本図の❶に示すように、クライアント端末ＰＣ１０は、サーバ端末ＰＣ２０に対しドメイン（ホスト）名によりテルネット接続を行う場合、ルータ４０に対しＤＮＳの問い合わせを行う。

【００２８】本図の❷に示すように、ルータ４０は、ＤＮＳエントリーテーブルの表３にサーバ端末ＰＣ２０のエントリーが存在しない場合、ＤＮＳサーバ検索エントリーに従ってルータ５０に対しＤＮＳの問い合わせを行う。本図の❸に示すように、ルータ５０は、ドメイン名「ＰＣ２０」のＤＮＳの問い合わせを受信するとＤＳＮエントリーテーブルの表４に「ＰＣ２０」のエントリーが存在するため、ルータ４０に対してＤＮＳの返答を行う。ＤＮＳの応答においては、ドメイン名「ＰＣ２０」とグローバルＩＰアドレスｃ．ｃ．ｃ．ｃの組み合わせではなく、予約ホスト名「サーバ０１」とグローバルＩＰアドレスｃ．ｃ．ｃ．ｃの組み合わせで返答する。

【００２９】本図の❹に示すように、ルータ４０はＤＮＳの返答を受信すると、ＤＮＳメッセージヘッダのＩｄｅｎｔｉｆｉｃａｔｉｏｎ（識別）フィールドを確認することにより、「ＰＣ２０」で問い合わせたものに対し、「サーバ０１」で返答を受信したことを認識する。この時点で、ルータ４０は、表４のように、「ＰＣ２０」に対し、予約ホスト名「サーバ０１」のＤＮＳエントリーを追加する。次に、ルータ４０はクライアント端末ＰＣ１０に対してＤＮＳの返答を行う。ドメイン名は「ＰＣ２０」にして、ＩＰアドレスはルータ４０が収容しているプライベートネットワーク内で使用していないサブネットの中から任意のプライベートＩＰアドレス「ｘ．ｘ．ｘ．１」を入れてクライアント端末ＰＣ１０に返す。

【００３０】なお、ルータ４０からクライアント端末ＰＣ１０へのＤＮＳ応答は、ＤＮＳのキャシュ時間を「０」に設定する必要がある。これは、クライアント端末ＰＣ１０にある一定時間のキャシュ時間を与えると、この期間内はＤＮＳを使用せずにセッションを張りにくくることになり、ポート番号予約テーブルのエントリーが作成できないためである。

【００３１】

【表６】

ＲＴ４０のポート番号予約テーブル４０Ｃ

予約ホスト名	プライベートポート番号	内部予約ポート番号	仮IPアドレス	グローバルIPアドレス
サーバ01	—	２００１	x.x.x.1	c.c.c.c
	—	２００２	x.x.x.2	—
	—	２００３	x.x.x.3	—
	—	２００４	x.x.x.4	—
サーバ02	—	２００５	x.x.x.5	—
	—	２００６	x.x.x.6	—
	—	２００７	x.x.x.7	—
	—	２００８	x.x.x.8	—

【表７】

ＲＴ５０のポート番号予約テーブル５０Ｃ

予約ホスト名	プライベートポート番号	内部予約ポート番号	仮IPアドレス	グローバルIPアドレス
サーバ01	—	２００１	y.y.y.1	—
	—	２００２	y.y.y.2	—
	—	２００３	y.y.y.3	—
	—	２００４	y.y.y.4	—
サーバ02	—	２００５	y.y.y.5	—
	—	２００６	y.y.y.6	—
	—	２００７	y.y.y.7	—
	—	２００８	y.y.y.8	—

【表８】

ＲＴ４０のポート番号予約テーブル４０Ｃ

（テルネット（ＳＹＮ）受信後）

予約ホスト名	プライベートポート番号	内部予約ポート番号	仮IPアドレス	グローバルIPアドレス
サーバ01	１０２４	２００１	x.x.x.1	c.c.c.c
	—	２００２	x.x.x.2	—
	—	２００３	x.x.x.3	—
	—	２００４	x.x.x.4	—
サーバ02	—	２００５	x.x.x.5	—
	—	２００６	x.x.x.6	—
	—	２００７	x.x.x.7	—
	—	２００８	x.x.x.8	—

【００３２】上記の表６、７のポート番号予約テーブルついては、全ルータ４０、５０に実装する必要がある。表６、７は予約ホスト名、プライベートポート番号、内部予約ポート番号、仮ＩＰアドレス、グローバルＩＰアドレスで構成されている。上記の予約ホスト名は、前述のように、予め取り決めておくサーバのホスト名であり、全てのルータ４０、５０で統一が取れている必要がある。上記のプライベートポート番号はルータ４０、５０のプライベートネットワーク１００、２００内のクライアント端末ＰＣ１０、サーバ端末ＰＣ２０、サーバ端末ＰＣ２１が任意のパケットを送信する際の送信元ポート番号が入る（後述参照）。

【００３３】上記の内部予約ポート番号は予め取り決めておく送信元のポート番号であり、全てのルータ４０、５０で統一がとれている必要がある。例えば、表６、７、８に示す内部予約ポート番号「２００１」、「２００２」、「２００３」、「２００４」は予約ホスト名「サーバ０１」を特定し、内部予約ポート番号「２００５」、「２００６」、「２００７」、「２００８」は予約ホスト名「サーバ０２」を特定する。上記の仮ＩＰアドレスは、送信先の任意のプライベートＩＰアドレスを割り与える。内部予約ポート番号と、仮ＩＰアドレスの対応付けは、後述するように、管理される。上記ＤＮＳの問い合わせによるプライベートＩＰアドレスは一時的に割り与えるもので仮ＩＰアドレスとして使用される。この場合、ルータ４０はポート番号予約テーブルの表６を更新する。

【００３４】ルータ４０では、表６、８に示すように、内部予約ポート番号「２００１」、「２００２」、「２００３」、「２００４」、「２００５」、「２００６」、「２００７」、「２００８」に対して、仮ＩＰアドレス「ｘ．ｘ．ｘ．１」、「ｘ．ｘ．ｘ．２」、「ｘ．ｘ．ｘ．３」、「ｘ．ｘ．ｘ．４」、「ｘ．ｘ．ｘ．５」、「ｘ．ｘ．ｘ．６」、「ｘ．ｘ．ｘ．７」、「ｘ．ｘ．ｘ．８」がそれぞれ対応つけられて管理される。ルータ５０では、表７に示すように、内部予約ポート番号「２００１」、「２００２」、「２００３」、「２００４」、「２００５」、「２００６」、「２００７」、「２００８」に対して、仮ＩＰアドレス「ｙ．ｙ．ｙ．１」、「ｙ．ｙ．ｙ．２」、「ｙ．ｙ．ｙ．３」、「ｙ．ｙ．ｙ．４」、「ｙ．ｙ．ｙ．５」、「ｙ．ｙ．ｙ．６」、「ｙ．ｙ．ｙ．７」、「ｙ．ｙ．ｙ．８」がそれぞれ対応つけて管理される。

【００３５】上記グローバルＩＰアドレスでは、仮ＩＰアドレスとして「ｘ．ｘ．ｘ．１」が設定されると、これに対応して、表６、８に示すように、ルータ４０のＩＰマスカレードで使用される送信先グローバルＩＰアドレス「ｃ．ｃ．ｃ．ｃ」が設定される。

【００３６】図４はＩＰマスカレード機能を使用しているルータ４０、５０のプライベートネットワーク間の転送を説明する図である。本図の①において、前述のように、ルータ４０からＤＮＳの返答を受信したクライアント端末ＰＣ１０は、パケットの送信先ＩＰアドレスを、ルータ４０が管理する仮ＩＰアドレス「ｘ．ｘ．ｘ．１」に設定し、送信元ポート番号を、１０２４以上に一例として１０２４に設定する。この場合、仮ＩＰアドレスとして「ｘ．ｘ．ｘ．１」が設定されると、これに対応して、表８に示すように、プライベートポート番号１０２４が設定される。

【００３７】パケットの送信先ポート番号を２３にしてテルネットセッションが開始される。つまり、テルネット接続要求（Ｔｅｌｎｅｔ（ＳＹＮ））が行われる。この時点で、ルータ４０は、表３（ｃ）に示すようにプライベートポート番号と内部予約ポート番号の対応が更新される。この場合、送信先ポートは、前述のように、ポート番号２３であり、これはｗｅｌｌ－ｋｎｏｗｎ ｐｏｒｔ（よく知られたポート）である。パケットの送信先プライベートＩＰアドレスは仮ＩＰアドレス「ｘ．

ｘ．ｘ．１」に設定され、送信元プライベートＩＰアドレスは「ａ．ａ．ａ．ａ」に設定される。

【００３８】本図の❷において、ルータ４０は、ポート番号予約テーブルの表６に従って、送信先のプライベートＩＰアドレスを仮ＩＰアドレス「ｘ．ｘ．ｘ．１」からグローバルＩＰアドレス「ｃ．ｃ．ｃ．ｃ」に変換し、且つ、送信元ポート番号をクライアント端末ＰＣ１０が設定してきたポート番号「１０２４」から内部予約ポート番号「２００１」に変更して、グローバルネットワーク側にパケットを送信する。また、送信元プライベートＩＰアドレスは「ａ．ａ．ａ．ａ」は送信元グローバルＩＰアドレス「ｂ．ｂ．ｂ．ｂ」に変更される。

【００３９】本図の❸において、グローバルネットワーク経由で本パケットを受信したルータ５０は、送信元ポート番号を確認し、ポート番号予約テーブル表７から送信元ポート番号が「２００１」であることからサーバ端末ＰＣ２０宛てのパケットであることが分かったため、サーバ端末ＰＣ２０に対してパケットを送信する。また、送信先グローバルＩＰアドレス「ｃ．ｃ．ｃ．ｃ」が送信先プライベートＩＰアドレス「ｄ．ｄ．ｄ．ｄ」に変換される。サーバ端末ＰＣ２０から端子ＰＣ１０への返りのパケットは、端末ＰＣ１０から端末ＰＣ２０へのパケット送信と逆の変換を行うことにより可能になる（本図❹、❺、❻参照）。上記例の続きとして、テルネットの接続要求に対する応答確認（Ｔｅｌｎｅｔ（ＡＣＫ／ＳＹＮ））を行う。

【００４０】但し、ルータ５０は、本来ならばＩＰマスカレード機能によってプライベートネットワーク側のサーバ端末ＰＣ２０からパケットを受信した場合、送信元ポート番号を変更するが、送信元ポート番号がよく知られたポート（ｗｅｌｌ－ｋｎｏｗｎ　ｐｏｒｔ（例えば、２３番））である場合は、ポート番号を変更しないようにする。この一連の処理によって、予約ホスト名、プライベートポート番号、内部予約ポート番号、仮ＩＰアドレス、グローバルＩＰアドレスの一連のエントリーを完成させることができ、ＩＰマスカレード機能を使用しているルータ４０、５０のプライベートネットワーク間で、パケットの転送が可能になる。なお、ポート番号予約テーブルのエントリー削除は、タイマによって行う。ある一定期間エントリーを使用しなかった場合、該当エントリーは削除される。不使用エントリーの堆積に起因する処理煩雑を避けるためである。

【００４１】

【発明の効果】以上説明したように、本発明によれば、ＩＰマスカレード機能によりプライベートネットワークからインターネットへの同時接続時には１つのグローバルＩＰアドレスがあればよく、ポート番号予約テーブルを参照することによりインターネットからプライベートネットワークへの同時接続時にも１つのグローバルＩＰアドレスがあればよいので、グローバルＩＰアドレスの有効活用が可能である。また、広域ネットワークを介してインターネット、イントラネットへの同時接続は、広域ネットワーク回線の１チャンネルのみの契約で可能になる。

【図面の簡単な説明】

【図１】図１は本発明に係るＩＰマスカレードによるネットワーク構成を示す図である。

【図２】図２はルータ４０、５０のＤＨＣＰ機能を説明する図である。

【図３】図３はルータ４０、５０のＤＮＳ機能を説明する図である。

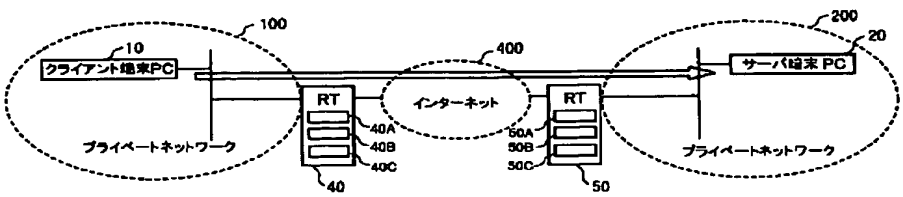
【図４】図４はＩＰマスカレード機能を使用しているルータ４０、５０のプライベートネットワーク間の転送を説明する図である。

【図５】図５は従来の従来のＩＰマスカレードによるプライベートネットワーク間接続システムを説明する図である。

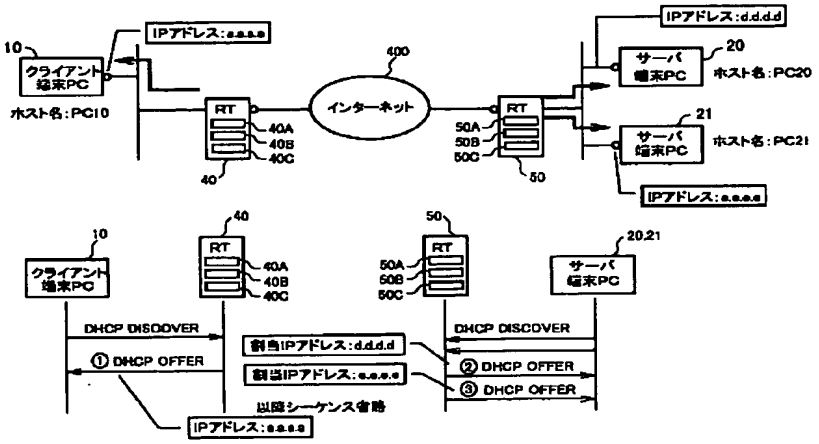
【符号の説明】

１０…クライアント端末ＰＣ
２０、２１…サーバ端末ＰＣ
４０、５０…ルータ
４０Ａ…ルータ４０のＤＨＣＰエントリーテーブル
４０Ｂ…ルータ４０のＤＮＳエントリーテーブル
４０Ｃ…ルータ４０のポート番号予約テーブル
５０Ａ…ルータ５０のＤＨＣＰエントリーテーブル
５０Ｂ…ルータ５０のＤＮＳエントリーテーブル
５０Ｃ…ルータ５０のポート番号予約テーブル
１００、２００…プライベートネットワーク
３００…広域ネットワーク
４００…インターネット

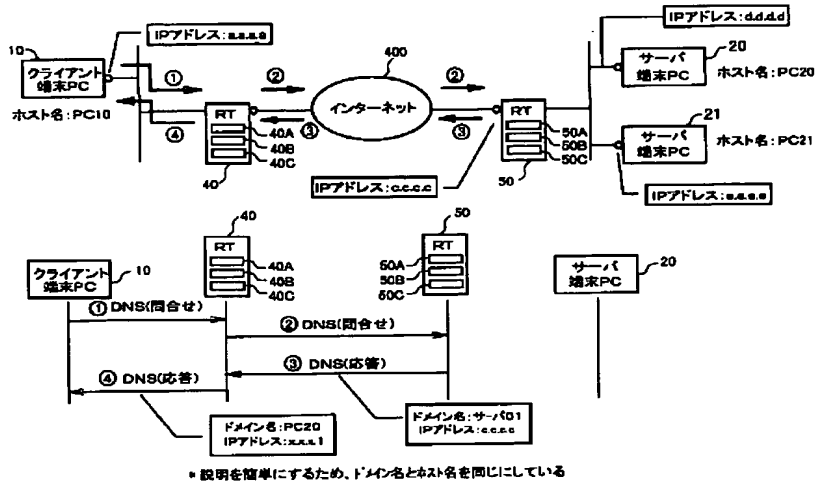
【図１】



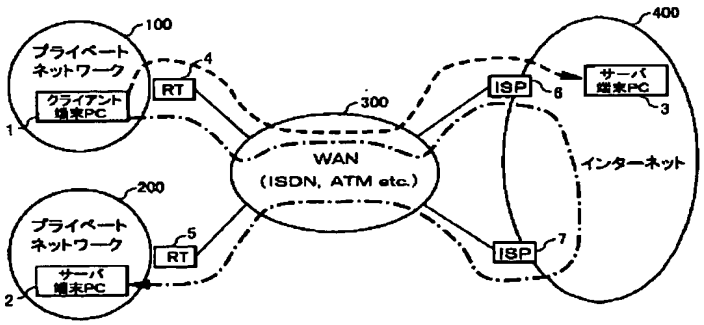
【図2】


IPアドレス:d.d.d.d
10
クライアント端末PC
IPアドレス:a.a.a.a
400
インターネット
20
サーバ端末PC
ホスト名:PC20
ホスト名:PC10
RT
40A
40B
40C
40
50A
50B
50C
50
21
サーバ端末PC
ホスト名:PC21
IPアドレス:e.e.e.e
20.21
DHCP DISCOVER
① DHCP OFFER
割当IPアドレス:d.d.d.d
割当IPアドレス:e.e.e.e
② DHCP OFFER
③ DHCP OFFER
以降シーケンス省略

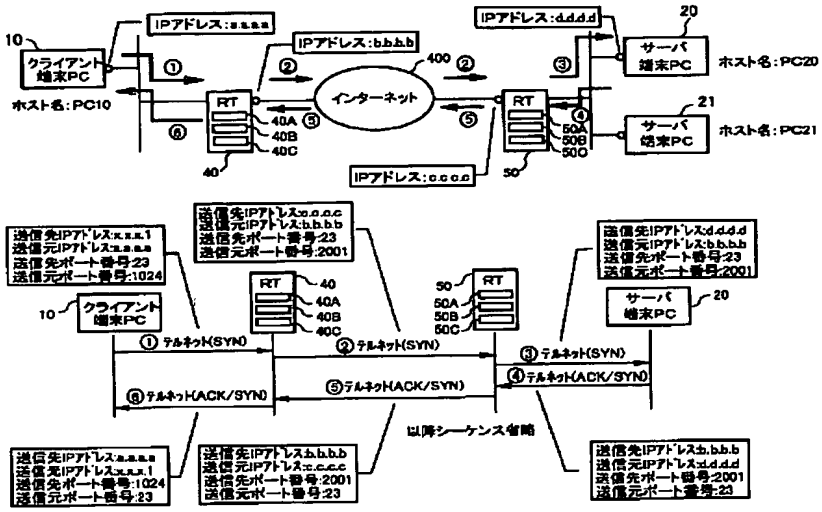
【図3】


IPアドレス:d.d.d.d
IPアドレス:a.a.a.a
10
クライアント端末PC
ホスト名:PC10
400
インターネット
20
サーバ端末PC
ホスト名:PC20
RT
40A
40B
40C
40
50A
50B
50C
50
21
サーバ端末PC
ホスト名:PC21
IPアドレス:c.c.c.c
IPアドレス:e.e.e.e
① DNS(問合せ)
② DNS(問合せ)
③ DNS(応答)
④ DNS(応答)
ドメイン名:PC20
IPアドレス:x.x.x.1
ドメイン名:サーバ01
IPアドレス:c.c.c.c
* 説明を簡単にするため、ドメイン名とホスト名を同じにしている

【図5】


100
プライベートネットワーク
クライアント端末PC
1
RT
4
300
WAN
(ISDN, ATM etc.)
200
プライベートネットワーク
サーバ端末PC
2
RT
5
ISP
6
ISP
7
400
サーバ端末PC
3
インターネット

【図4】


10
クライアント端末PC
ホスト名:PC10
IPアドレス:a.a.a.a
IPアドレス:b.b.b.b
IPアドレス:c.c.c.c
IPアドレス:d.d.d.d
400
インターネット
RT
40
40A
40B
40C
50
50A
50B
50C
20
サーバ端末PC
ホスト名:PC20
21
サーバ端末PC
ホスト名:PC21
①
②
③
④
⑤
⑥
送信先IPアドレス:a.a.a.a
送信元IPアドレス:x.x.x.1
送信先ポート番号:1024
送信元ポート番号:23
送信先IPアドレス:c.c.c.c
送信元IPアドレス:b.b.b.b
送信先ポート番号:23
送信元ポート番号:2001
送信先IPアドレス:d.d.d.d
送信元IPアドレス:b.b.b.b
送信先ポート番号:23
送信元ポート番号:2001
①テルネット(SYN)
②テルネット(SYN)
③テルネット(SYN)
④テルネット(ACK/SYN)
⑤テルネット(ACK/SYN)
⑥テルネット(ACK/SYN)
以降シーケンス省略
送信先IPアドレス:a.a.a.a
送信元IPアドレス:x.x.x.1
送信先ポート番号:1024
送信元ポート番号:23
送信先IPアドレス:b.b.b.b
送信元IPアドレス:c.c.c.c
送信先ポート番号:2001
送信元ポート番号:23
送信先IPアドレス:b.b.b.b
送信元IPアドレス:d.d.d.d
送信先ポート番号:2001
送信元ポート番号:23